enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

IT

Da gennaio 2019 ad aprile 2020

Cyber-spionaggio

Panorama delle minacce analizzato dall'ENISA

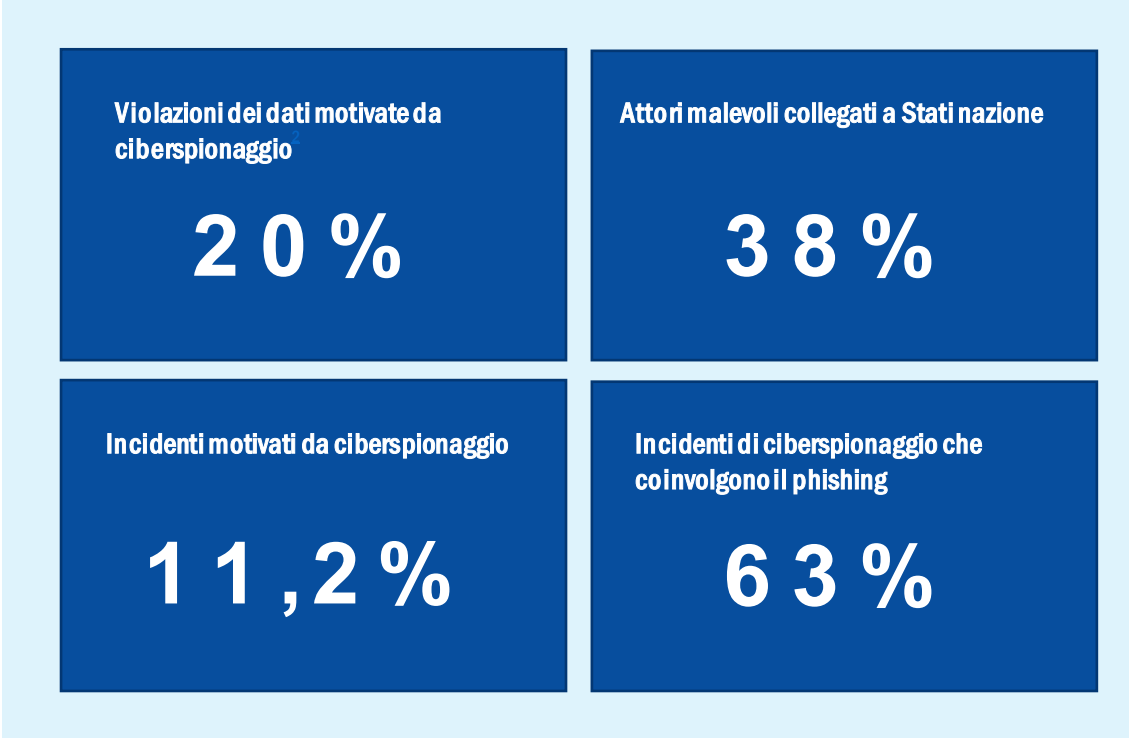
Quadro generale

Il ciberspionaggio è considerato sia una minaccia sia un movente nel programma della sicurezza informatica. È definito come «l'uso di reti informatiche per ottenere accesso illecito a informazioni riservate, in genere detenute da un governo o da un'altra organizzazione».[1]

Nel 2019 molti rapporti hanno rivelato che le organizzazioni globali considerano il ciberspionaggio (o spionaggio sponsorizzato da Stati nazione) una minaccia crescente che interessa i settori industriali, così come le infrastrutture critiche e strategiche in tutto il mondo, compresi i ministeri governativi, le ferrovie, i fornitori di telecomunicazioni, le aziende energetiche, gli ospedali e le banche. Il ciberspionaggio si concentra sulla determinazione della geopolitica e sul furto di segreti di Stato e commerciali, diritti di proprietà intellettuale e informazioni di proprietà riservata in campi strategici. Mobilita inoltre attori dell'economia, dell'industria e dei servizi di intelligence stranieri, nonché gli attori che lavorano per conto dei medesimi. In un recente rapporto, gli analisti di intelligence sulle minacce non si sono sorpresi nel rilevare che il 71% delle organizzazioni tratta il ciberspionaggio e altre minacce come una «scatola nera» e sta ancora apprendendo le prime nozioni.

Nel 2019 **è aumentato il numero di attacchi informatici promossi da Stati nazione mirati all'economia e il trend è probabilmente destinato a continuare.** Nel dettaglio, gli attacchi all'Internet degli oggetti industriale (Industrial Internet of Things, IIoT), promossi da Stati nazione e altri attacchi guidati da avversari sono in aumento nei settori dei servizi pubblici, del petrolio e del gas naturale e della produzione. Inoltre, gli attacchi informatici condotti da gruppi di minacce persistenti avanzate (Advanced Persistent Threat, APT) indicano che gli attacchi finanziari sono spesso motivati dallo spionaggio. Utilizzando tattiche, tecniche e procedure (TTP) simili a quelle dei loro omologhi di spionaggio, gruppi come Cobalt Group, Carbanak e FIN7 sono riusciti presumibilmente a colpire grandi istituzioni finanziarie e catene di ristoranti.

- La Commissione per gli affari esteri del Parlamento europeo ha invitato gli Stati membri a istituire un'unità di ciberdifesa e a lavorare insieme per la difesa comune. Ha affermato che «l'ambiente strategico dell'Unione è andato deteriorandosi [...] per fare fronte alle molteplici sfide che, direttamente o indirettamente, incidono sulla sicurezza dei suoi Stati membri e dei suoi cittadini; che le questioni che incidono sulla sicurezza dei cittadini dell'Unione comprendono conflitti armati immediatamente a Est e a Sud del continente europeo e Stati fragili, terrorismo - in particolare jihadismo - attacchi informatici e campagne di disinformazione, ingerenze straniere nei processi politici ed elettorali europei».[42]
- Gli attori delle minacce, motivati da un guadagno di natura economica, politica o ideologica, concentreranno sempre più gli attacchi sulle reti di fornitori con programmi di cibersicurezza deboli. Gli avversari del ciberspionaggio hanno lentamente spostato i loro modelli di attacco verso lo sfruttamento di partner della catena di fornitura di terze e quarte parti.[1]



Incidenti

- Il Ministero della difesa nazionale della Corea del Sud ha annunciato che ignoti hacker avevano compromesso i sistemi informatici dell'ufficio acquisti del ministero.[3]
- Il Dipartimento di giustizia degli Stati Uniti ha annunciato un'operazione promossa da uno Stato straniero con una botnet destinata a provocare l'interruzione dei servizi prendendo di mira aziende dei settori dei media, aerospaziale, finanziario e delle infrastrutture critiche.[16]
- La società di software norvegese Visma ha rivelato di essere stata presa di mira da hacker che hanno tentato di sottrarre segreti commerciali ai clienti dell'azienda.[4]
- Alcuni soggetti sono stati sorpresi nelle prime fasi di un tentativo di accedere ai sistemi informatici di diversi partiti politici e del Parlamento federale australiano.[17]
- La società aerospaziale europea Airbus ha rivelato di essere stata oggetto di un attacco di presunti hacker sponsorizzati da Stati nazione, che hanno rubato dati personali e informazioni di identificazione IT di molti dipendenti.[19]
- A seguito di un attacco alle forze militari indiane nel Kashmir, hacker pakistani hanno colpito quasi 100 siti web e sistemi critici del governo indiano.[5]
- La commissione elettorale nazionale indonesiana ha riferito che soggetti cinesi e russi si erano introdotti nella banca dati degli elettori prima delle elezioni presidenziali e legislative nel paese.[20]
- Hacker stranieri hanno preso di mira diverse agenzie pubbliche europee prima delle elezioni dell'UE di maggio[21]
- L'agenzia australiana responsabile dell'intelligence dei segnali, Australian Signals Directorate, ha rivelato di avere condotto attacchi informatici contro l'ISIS in Medio Oriente.[22]
- La polizia finlandese ha indagato su un attacco DoS diretto contro il servizio web utilizzato per pubblicare i conteggi dei voti delle elezioni in Finlandia.[6]
- L'ufficio di Hong Kong di Amnesty International ha annunciato di essere stato vittima di un attacco informatico.[23]
- Le forze di difesa israeliane hanno lanciato un attacco aereo su Hamas, dopo che quest'ultimo aveva tentato invano di hackerare obiettivi israeliani.[7]

- Una rete iraniana di siti web e account è stata presumibilmente utilizzata per diffondere informazioni false su Stati Uniti, Israele e Arabia Saudita.[24]
- Agenzie governative croate sono state prese di mira in una serie di attacchi da parte di hacker sponsorizzati da Stati non identificati. I payload del malware erano la backdoor Empire e SilentTrinity, nessuno dei quali era stato osservato in precedenza.[26]
- In Libia sono stati arrestati due uomini accusati di lavorare con una «troll farm» russa per influenzare le elezioni in diversi paesi africani.[27]
- Diverse importanti aziende industriali tedesche, tra cui BASF, Siemens ed Henkel, hanno annunciato di essere state vittime di una campagna di hacking sponsorizzata da Stati.[28]
- Un gruppo sponsorizzato da Stati avrebbe condotto una serie di attacchi informatici contro giornalisti, accademici, avvocati, attivisti dei diritti umani e politici egiziani.[8]
- Un gruppo di hacker sponsorizzato da Stati ha preso di mira diplomatici e utenti russofoni di alto profilo nell'Europa orientale utilizzando un malware denominato Attor.[29]
- È stato scoperto che una società israeliana di cibersicurezza aveva venduto spyware utilizzati per colpire alti funzionari governativi e militari in almeno 20 paesi, sfruttando una vulnerabilità in WhatsApp.[32]
- È stato rivelato che una campagna della durata di 7 anni, condotta da un gruppo di spionaggio di lingua spagnola non identificato, ha condotto al furto di file di mappatura sensibili sottratti ad alti funzionari dell'esercito venezuelano.[10]
- Un gruppo di ciberspionaggio sponsorizzato da Stati avrebbe condotto una campagna di phishing, rivolta ad agenzie governative e imprese statali cinesi, per acquisire informazioni relative a scambi economici, questioni di difesa e relazioni estere.[33]
- Il Ministero degli esteri ceco è stato vittima di un attacco informatico a opera di uno Stato straniero non specificato.[34]
- Un attore non statale ha preso di mira il partito laburista britannico con un importante attacco DDoS, che ha temporaneamente messo fuori uso i sistemi informatici del partito prima delle elezioni nazionali.[36]

Incidenti

Il caso General Electric

Xiaoqing Zheng, cittadino americano di origine cinese, è stato accusato di spionaggio ai danni della General Electric (GE). Zheng avrebbe rubato i segreti della tecnologia delle turbine della GE e li avrebbe consegnati a un uomo d'affari cinese che, a sua volta, li avrebbe consegnati a funzionari cinesi. Zheng ha lavorato per la GE tra il 2008 e il 2018.[15]

Il dipartimento di giustizia degli Stati Uniti ha accusato i due uomini del furto di informazioni per promuovere i loro interessi commerciali in due società di ricerca e sviluppo di turbine, Liaoning Tianyi Aviation Technology Co Ltd e Nanjing Tianyi Avi Tech Co Ltd.[47]

Il *modus operandi* di questo attore interno comprendeva:

- la copia dei segreti su una chiavetta USB fino a quando GE non ha bloccato l'uso di questi dispositivi;
- la cifratura dei segreti e il ricorso alla steganografia per nascondere i file di dati nel codice binario di file di foto digitali;
- il collegamento di un iPhone al desktop di lavoro per copiare l'immagine;
- l'invio dei file al suo indirizzo e-mail personale.

Misure di mitigazione

A causa della natura estesa di questa minaccia, diverse delle misure di mitigazione raccomandate in questa relazione per altre minacce potrebbero essere impiegate nell'ambito dei seguenti controlli di mitigazione di base[2]:

- Identificare i ruoli «mission critical» nell'organizzazione e stimarne l'esposizione ai rischi di spionaggio. Valutare tali rischi sulla base delle informazioni aziendali (ossia business intelligence).
- Creare politiche di sicurezza che contemplino controlli di sicurezza delle risorse umane, dell'azienda e delle operazioni per la mitigazione dei rischi. Queste dovrebbero includere regole e pratiche per la sensibilizzazione, la governance aziendale e le attività di sicurezza.
- Stabilire pratiche aziendali per comunicare, formare il personale sulle regole elaborate.
- Sviluppare criteri di valutazione (indicatori chiave di prestazione, KPI) per un benchmark dell'operazione e relativo adattamento ai cambiamenti imminenti.
- Creare una white list per i servizi applicativi critici in funzione del livello di rischio valutato.
- Valutare le vulnerabilità e installare regolarmente le patch del software, in particolare per i sistemi che si trovano sul perimetro.
- Implementare il principio della necessità di sapere (need-to-know) per la definizione dei diritti di accesso e stabilire controlli per monitorare l'uso improprio di profili con privilegi.
- Prevedere il filtraggio dei contenuti per tutti i canali in entrata e in uscita (ad esempio e-mail, web, traffico di rete).

Riferimenti bibliografici

1. «Cyber Threatscape Report. 2019.» IDefense - Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

2. «Data Breach Investigations Report 2020» DBR & Verizon. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report-emea.pdf

3. Catalin Cimpanu. «Hackers breach and steal data from South Korea's Defense Ministry» 16 gennaio 2019. ZDNet. https://www.zdnet.com/article/hackers-breach-and-steal-data-from-south-koreas-defense-ministry/

4. Jack Stubbs. «China hacked Norway's Visma to steal client secrets: investigators» 6 febbraio 2019. Reuters. https://www.reuters.com/article/us-china-cyber-norway-visma/china-hacked-norways-visma-to-steal-client-secrets-investigators-idUSKCN1PV141

5. Kate Fazzini. «In India-Pakistan conflict, there's a long-simmering online war, and some very good hackers on both sides». 28 febbraio 2019. CNBC. https://www.cnbc.com/2019/02/27/india-pakistan-online-war-includes-hacks-social-media.html

6. Kati Pohjanpalo. «Finland Detects Cyber Attack on Online Election-Results Service». 10 aprile 2019. Bloomberg.

https://www.bloomberg.com/news/articles/2019-04-10/finland-detects-cyber-attack-on-online-election-results-service

7. Lily Hay Newman «What Israel's Strike on Hamas Hackers Means For Cyberwar» 5 giugno 2019. Wired. https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/

8. «Egypt Is Using Apps to Track and Target Its Citizens, Report Says» 3 ottobre 2019. The New York Times. https://www.nytimes.com/2019/10/03/world/middleeast/egypt-cyber-attack-phones.html

9. Colin Lencher. «Huawei accuses the US of 'launching cyber attacks' against the company» 4 settembre 2019. The Verge. https://www.theverge.com/2019/9/4/20849092/huawei-cyberattacks-us-government-netowrks-employee-harassment

10. Catalin Cimpanu «A cyber-espionage group has been stealing files from the Venezuelan military» 5 agosto 2019. ZDNet. https://www.zdnet.com/article/a-cyber-espionage-group-has-been-stealing-files-from-the-venezuelan-military/

11. Catalin Cimpanu. «Croatian government targeted by mysterious hackers» 5 luglio 2019. ZDNet. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

12. Michael McGowan. «China behind massive Australian National University hack, intelligence officials say» 6 giugno 2019. The Guardian. https://www.theguardian.com/australia-news/2019/jun/06/china-behind-massive-australian-national-university-hack-intelligence-officials-say

13. «General election 2019: Labour Party hit by second cyber-attack» 12 novembre 2019. BBC. https://www.bbc.com/news/election-2019-50388879

14. Nicole Perlroth, Matthew Rosenberg. «Russians Hacked Ukrainian Gas Company at Center of Impeachment» 13 gennaio 2020. The New York Times. https://www.nytimes.com/2020/01/13/us/politics/russian-hackers-burisma-ukraine.html

15. Danny Bradbury. «GE Engineer Charged for Novel Data Theft» 24 aprile 2019. Info Security. https://www.infosecurity-magazine.com/infosec/ge-engineer-charged-data-theft-1/

16. «U.S. announces disruption of 'Joanap' botnet linked with North Korea». 30 gennaio 2019. CyberScoop. https://www.cyberscoop.com/joanap-botnet-north-korea-department-of-justice/

17. «The cyber attack on Parliament was done by a 'state actor' — here's how experts figure that out». 20 febbraio 2019. ABC News. https://www.abc.net.au/news/2019-02-20/cyber-activists-or-state-actor-attack-how-experts-tell/10825466

18. «While Trump was meeting with Kim Jong Un in Vietnam, North Korean hackers reportedly attacked targets in the US». 5 marzo 2019. Business Insider. https://www.businessinsider.com/north-korean-hackers-trump-kim-meeting-mcafee-2019-3

19. «Airbus hit by series of cyber attacks on suppliers». 26 settembre 2019. France 24. https://www.france24.com/en/20190926-airbus-hit-by-series-of-cyber-attacks-on-suppliers

20. «Indonesia Says Election Under Attack From Chinese, Russian Hackers». 12 marzo 2019. Bloomberg. https://www.bloomberg.com/news/articles/2019-03-12/indonesia-says-poll-under-attack-from-chinese-russian-hackers

21. «Cyber-espionage warning: Russian hacking groups step up attacks ahead of European elections». 21 marzo 2019. ZDNet. https://www.zdnet.com/article/cyber-espionage-warning-russian-hacking-groups-step-up-attacks-ahead-of-european-elections/

22. «Australian cyber soldiers hacked Islamic State and crippled its propaganda unit – here's what we know». 18 dicembre 2019. ABC News. https://www.abc.net.au/news/2019-12-18/inside-the-secret-hack-on-islamic-state-propaganda-network/11809426

23. «State-sponsored hackers target Amnesty International Hong Kong with sophisticated cyber-attack». 25 aprile 2019. Amnesty International. https://www.amnesty.org/en/latest/news/2019/04/state-sponsored-cyber-attack-hong-kong/

24. «New Report Shows How a Pro-Iran Group Spread Fake News Online». 14 maggio 2019. The New York Times. https://www.nytimes.com/2019/05/14/world/middleeast/iran-fake-news-report.html

25. «China behind massive Australian National University hack, intelligence officials say». 6 giugno 2019. The Guardian. https://www.theguardian.com/australia-news/2019/jun/06/china-behind-massive-australian-national-university-hack-intelligence-officials-say

26. «Croatian government targeted by mysterious hackers». 5 luglio 2019. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

27. «Two Russians accused of election interference arrested in Libya». 8 luglio 2019. Cyber Scout. https://cyberscout.com/en/blog/two-russians-accused-of-election-interference-arrested-in-libya

28. «BASF, Siemens, Henkel, Roche target of cyber attacks». 24 luglio 2019. Reuters. https://www.reuters.com/article/us-germany-cyber/basf-siemens-henkel-roche-target-of-cyber-attacks-idUSKCN1UJ147

29. «New espionage malware found targeting Russian-speaking users in Eastern Europe» 10 ottobre 2019. ZDNet. https://www.zdnet.com/article/new-espionage-malware-found-targeting-russian-speaking-users-in-eastern-europe/

30. «Advanced Israeli spyware is targeting Moroccan human rights activists». Novembre 2019. The NextWeb. https://thenextweb.com/security/2019/10/14/advanced-israeli-spyware-is-targeting-moroccan-human-rights-activists/

31. «Hacking the hackers: Russian group hijacked Iranian spying operation, officials say». 21 ottobre 2019. Reuters. https://www.reuters.com/article/us-russia-cyber/hacking-the-hackers-russian-group-hijacked-iranian-spying-operation-officials-say-idUSKBN1X00AK

32. «Israeli spyware allegedly used to target Pakistani officials' phones». 19 dicembre 2019. The Guardian. https://www.theguardian.com/world/2019/dec/19/israeli-spyware-allegedly-used-to-target-pakistani-officials-phones

33. «A phishing campaign with nation-state hallmarks is targeting Chinese government agencies». 8 agosto 2019. Cyber Scoop. https://www.cyberscoop.com/china-phishing-anomali-nation-state-apt/

34. «Foreign power was behind cyber attack on Czech ministry: Senate». 13 agosto 2019. Reuters. https://www.france24.com/en/20190926-airbus-hit-by-series-of-cyber-attacks-on-suppliers

35. «Huawei technicians helped government officials in two African countries track political rivals and access encrypted communications». 15 agosto 2019. The Wall Street Journal. https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017

36. «Labour suffers second cyber-attack in two days» 12 novembre 2019. The Guardian. https://www.theguardian.com/politics/2019/nov/12/labour-reveals-large-scale-cyber-attack-on-digital-platforms

37. «Extensive hacking operation discovered in Kazakhstan». 23 novembre 2019. ZDNet. https://www.zdnet.com/article/extensive-hacking-operation-discovered-in-kazakhstan/

Riferimenti bibliografici

38. «A Notorious Iranian Hacking Crew Is Targeting Industrial Control Systems». 20 novembre 2019. Wired. https://www.wired.com/story/iran-apt33-industrial-control-systems/

39. «Russian 'Gamaredon' Hackers Back at Targeting Ukraine Officials». 6 dicembre 2019. Security Week. https://www.securityweek.com/russian-gamaredon-hackers-back-targeting-ukraine-officials

40. «Iran announced it foiled 'really massive' foreign cyber attack». 11 dicembre 2019. Security Affairs. https://securityaffairs.co/wordpress/94981/cyber-warfare-2/iran-foreign-cyber-attack.html

41. «Croatian government targeted by mysterious hackers». 5 luglio 2019. ZDNet. https://www.zdnet.com/article/croatian-government-targeted-by-mysterious-hackers/

42. «Relazione sull'attuazione della politica estera e di sicurezza comune - Relazione annuale» 18 dicembre 2019. Parlamento europeo. https://www.europarl.europa.eu/doceo/document/A-9-2019-0054_IT.html

43. «Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent». 26 settembre 2012. Krebs on Security. https://www.belfercenter.org/publication/confronting-chinas-efforts-steal-defense-information

44. «Energy Manufacturer Also Victimized by IE Zero Day in Watering Hole Attack». 2 gennaio 2013. The Threat Post. https://threatpost.com/energy-manufacturer-also-victimized-ie-zero-day-watering-hole-attack-010213/77359/

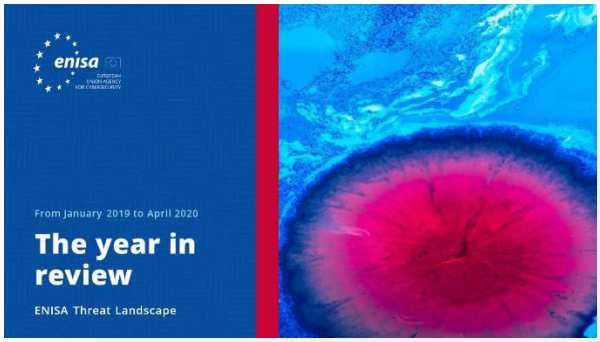
45. «The French Connection: French Aerospace-Focused CVE-2014-0322 Attack Shares Similarities with 2012 Capstone Turbine Activity». 25 febbraio 2014. CrowdStrike Blog. https://www.crowdstrike.com/blog/french-connection-french-aerospace-focused-cve-2014-0322-attack-shares-similarities-2012/

46. «Advanced Persistent Threat Groups». Fireeye. https://www.fireeye.com/current-threats/apt-groups.html

47. «U.S. accuses pair of stealing secrets, spying on GE to aid China». 23 aprile 2019. Reuters. https://www.reuters.com/article/us-usa-justice-ge/us-accuses-pair-of-stealing-secrets-spying-on-ge-to-aid-china-idUSKCN1RZ24O


«Nel corso del 2019 è aumentato il numero di attacchi informatici sponsorizzati da Stati nazione mirati all'economia».
in ETL 2020

Correlati



Relazione sul panorama delle minacce dell'ENISA **L'anno in rassegna**

Una sintesi delle tendenze nella cibersicurezza per il periodo tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA
Elenco delle prime 15 minacce

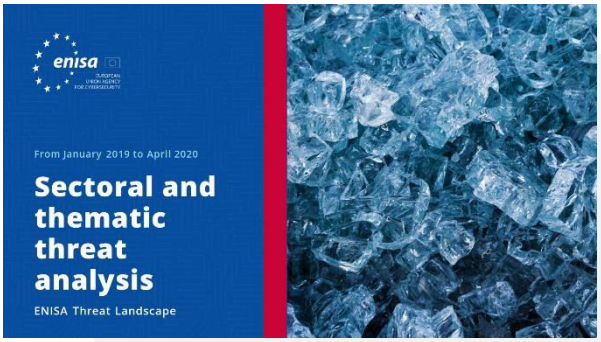
Elenco stilato dall'ENISA delle prime 15 minacce nel periodo tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA
Argomenti di ricerca

Raccomandazioni su argomenti di ricerca di vari quadranti nella cibersicurezza e nell'intelligence sulle minacce informatiche.

LEGGI LA RELAZIONE



Relazione sul panorama delle minacce dell'ENISA **Analisi delle minacce settoriali e tematiche**

Analisi contestualizzata delle minacce tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA **Tendenze emergenti**

Principali tendenze nella cibersicurezza osservate tra gennaio 2019 e aprile 2020.

LEGGI LA RELAZIONE

Relazione sul panorama delle minacce dell'ENISA
Quadro generale dell'intelligence sulle minacce informatiche

Situazione attuale dell'intelligence sulle minacce informatiche nell'UE.

LEGGI LA RELAZIONE

Informazioni

_ L'agenzia

L'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, è l'agenzia dell'Unione impegnata a conseguire un elevato livello comune di cibersicurezza in tutta Europa. Istituita nel 2004 e consolidata dal regolamento UE sulla cibersicurezza, l'Agenzia dell'Unione europea per la cibersicurezza contribuisce alla politica dell'UE in questo campo, aumenta l'affidabilità dei prodotti, dei servizi e dei processi TIC con sistemi di certificazione della cibersicurezza, coopera con gli Stati membri e gli organismi dell'UE e aiuta l'Europa a prepararsi per le sfide informatiche di domani. Attraverso lo scambio di conoscenze, lo sviluppo di capacità e la sensibilizzazione, l'Agenzia collabora con i suoi principali portatori di interessi per rafforzare la fiducia nell'economia connessa, aumentare la resilienza delle infrastrutture dell'Unione e, in ultima analisi, garantire la sicurezza digitale della società e dei cittadini europei. Maggiori informazioni sull'ENISA e sulle sue attività sono disponibili al seguente indirizzo: www.enisa.europa.eu.

Autori

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) e *tutti i componenti del gruppo di portatori di interessi sulla CTI dell'ENISA:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) e Thomas Hemker.

Redattori

Marco Barros Lourenço (ENISA) e Louis Marinos (ENISA).

Contatti

Per informazioni sul documento, si prega di contattare il seguente indirizzo press@enisa.europa.eu.
Per richieste dei media sul documento, si prega di contattare il seguente indirizzo press@enisa.europa.eu.

Saremmo lieti di ricevere il vostro feedback su questa relazione.
Dedicate un momento alla compilazione del questionario. Per accedere al modulo, fare clic qui.

Avvertenza legale

Si rammenta che, salvo diversamente indicato, la presente pubblicazione riflette l'opinione e l'interpretazione dell'ENISA. La presente pubblicazione non deve intendersi come un'azione legale intrapresa dall'ENISA o da suoi organi, a meno che non venga adottata ai sensi del regolamento (UE) N. 526/2013. La presente pubblicazione non rappresenta necessariamente lo stato dell'arte e l'ENISA si riserva il diritto di aggiornarla di volta in volta.

Secondo necessità, sono state citate anche fonti di terze parti. L'ENISA non è responsabile del contenuto delle fonti esterne, quali i siti web esterni riportati nella presente pubblicazione.

La presente pubblicazione è unicamente a scopo informativo. Deve essere accessibile gratuitamente. L'ENISA, o chiunque agisca in suo nome, declina ogni responsabilità per l'uso che può essere fatto delle informazioni di cui alla presente pubblicazione.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grecia
Tel.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu